TRANSLATION OF CITATION 4 (JP No. H8-314805)

[Embodiment]

Hereafter, a preferred embodiment of the present invention, as illustrated in the attached drawings, will be more specifically described. Fig. 1 is a general view of a wireless portable terminal system of the present invention. Fig. 2 is a block diagram illustrating a hardware configuration of the wireless portable terminal employed in the present invention. Fig. 3 is a sequence diagram describing an operation of a first embodiment of the present invention. Fig. 4 is a sequence diagram describing an operation of a second embodiment of the present invention.

First, a hardware configuration of the wireless portable terminal employed in the present invention will be described with reference to Fig. 2.

The wireless portable terminal comprises CPU 21 for controlling the entire system, ROM 24 in which a control program or the like is stored, work RAM 22 used by the control program, data storage RAM 23 in which personal data such as an address book, schedule or the like is stored, display 25 for displaying information, operations or the like, input device 26 for inputting data and wireless module 27 for conducting wireless control.

Data input by the input device 26 is stored in the data storage RAM 23.

Since the data storage RAM 23 is normally battery-protected, data stored in RAM 23 is not deleted even when mains power is turned off. In order to transmit data by radio, data is sent from the RAMs 22 and 23 and ROM 24 to the wireless module 27 via a system bus, whereby the data is transmitted.

Next, an overall configuration of the wireless portable terminal system will be described with reference to Fig. 1.

It is assumed here that an unauthorized third party is trying to use the wireless portable terminal 11. The wireless portable terminal 11 is registered at and managed by the information center 13 so that the information center 13 connected to wire network 14 via wireless station 19 can be accessed.

Next, an operation of the first embodiment of the present invention will be explained by means of the sequence diagram of Fig. 3.

It is now assumed that an unauthorized third party has tried entering a password to gain unauthorized access to the wireless portable terminal 11, and has caused input errors a specified number of times. At this time, the wireless portable

terminal 11 determines that the terminal 11 is a target of unauthorized use and sends an unauthorized use notification message to the information center 13. [301]

Upon receiving the unauthorized use notification message, the information center 13 sends a system data dump request message in order to make a backup copy of internal data of the wireless portable terminal 11. [302]

Key data for encrypting the system data of the wireless portable terminal 11 is added to the message. Upon receiving the message, the wireless portable terminal side first sends a system data dump start message and starts transmitting the internal data. [303]

In order to prevent the internal data from being illegally obtained by radio, the internal data is encrypted with an encryption key sent from the information center 13.

The system data of the wireless portable terminal 11 is sent packet by packet and the information center 13 sends to the wireless portable terminal 11 a reception confirmation message for each packet received. [304]

After making a backup copy, the information center 13 sends a system lock request message to the wireless portable terminal 11. Upon receiving the message, the wireless portable terminal 11 sends a system lock completion message, deletes the internal data, renders the wireless portable terminal unavailable and locks the terminal. [305 – 306]

A sequence diagram of Fig. 4 describes an operation of a second embodiment of the present invention, wherein the information center detects that a password input error has been made a specified number of times. According to the second embodiment, the information center 13 determines whether an unauthorized use of the wireless portable terminal 11 has occurred, which makes it unnecessary to transmit an unauthorized use notification message from the wireless portable terminal 11 to the information center 13. Otherwise, the operation of the second embodiment is exactly the same as that of the first embodiment and therefore, to avoid overlapping descriptions, will not be described here.